A Reconfigurable Scan Network based IC Identification for Embedded Devices

Omid Aramoon, Xi Chen, and Gang Qu
Department of Electrical and Computer Engineering and Institute for Systems Research
University of Maryland, College Park, USA
Email: {oaramoon, xchen128, gangqu}@umd.edu

***Abstract*— Most of the Internet of Things (IoT) and embedded devices are resource constrained, making it impractical to secure them with the traditional computationally expensive crypto-based solutions. However, security and privacy are crucial in many IoT applications such as health monitoring. In this paper, we consider one of the most fundamental security problems: how to identify and authenticate an embedded device. We consider the fact that embedded devices are designed by reusing IP cores with reconfigurable scan network (RSN) as the standard testing facility and propose to generate unique integrated circuit (IC) identifications (IDs) based on different configurations for the RSN. These circuit IDs not only solve the IC and device identification and authentication problems, they can also be considered as a lightweight security primitive in other applications such as IC metering and IP fingerprinting. We demonstrate through the ITC'02 benchmarks that the proposed approach can easily create from 10^7 to 10^{186} unique IDs without any overhead. Finally, our method complies with the IEEE standards and thus has high practical value.**

Keywords*— *device identification, lightweight authentication, IoT, reconfigurable scan chain, digital fingerprint, hardware security primitives.

I. INTRODUCTION

The notion of embedded systems has been around for about half a century and it boomed in the late 1990's when the embedded devices were networked. With the continuing advances and the convergence of multiple technologies, ranging from wireless communication to the Internet and from embedded systems to micro-electromechanical systems, the Internet of Things (IoT) emerged in the last decade in the form of large volumes of embedded devices connected by the Internet infrastructure to perform specific applications. Since then, IoT has been growing with an unprecedented pace and found applications in medical and healthcare monitoring, smart home and building surveillance, as well as in nation-wide infrastructures such as power grid, transportation systems, and environmental monitoring systems.

Security and privacy are among the key concerns for the development of IoT applications. It is pointed out that both the IoT and its Things are developed rapidly without appropriate consideration of the profound security challenges involved and the regulatory changes that might be necessary [1,2]. A January 2014 article in Forbes listed many Internet-connected appliances that can already "spy on people in their own homes" including televisions, kitchen appliances, cameras, and thermostats [3]. Embedded devices in automobiles such as brakes, engine, locks, hood and truck releases, horn, heat, and dashboard have been shown to be vulnerable to attackers who have access to the onboard network. The vehicle-to-vehicle and vehicle-to-infrastructure communication makes everyone's driving habit and daily commute routing public [4].

Mathematically strong and well-developed cryptographic techniques exist for all kinds of security related applications such as data encryption/decryption, user and devices authentication, secure computation and communication. Most of these crypto security primitives or protocols are (extremely) computationally expensive (for example, performing the modular exponentiation operation for large numbers of hundreds of bits). Unfortunately, in the IoT domains, the devices are extremely resource constrained and do not have the required computational power, memory, or (battery) power for such operations. As a result, in many IoT applications, both data and control communications, such as those between wearable/implantable medical devices and doctor or patient, are in plain text, which creates serious vulnerabilities.

In this paper, we propose a hardware security primitive as an alternative solution to the security of embedded and IoT devices. We utilize the testing infrastructure in these devices, which is compliant with IEEE 1149.1-2013 [5] and IEEE P1687 (IJTAG) [6], to create unique identifier at the circuit level for each device which can be verified through standard testing interface. More specifically, we adopt the reconfigurable scan network (RSN) and develop a fingerprint protocol to configure distinct RSN for each IC by utilizing the different connection styles between scan flip flops. The testing vector set will need to be modified consequently to reflect the different RSN configurations and thus can be used as IC identification (ID). In addition, these IDs can be used to fingerprint the design or intellectual property (IP), they can facilitate IP metering and tracking, they can also be used as the key for lightweight encryption and decryption.

978-3-9819263-0-9/DATE18/©2018 EDAA

Although the different connection styles in scan chain has been used in the literature for IP watermarking [22] and IP fingerprinting [16], they cannot be applied on embedded devices because these devices are typically designed by reusing IP cores and the scan chain information in each of the IP core, which is needed for [16] and [22], will not be available. In our approach, we take advantage of the fact that such devices are tested by RSN and create unique device IDs at RSN without going into the IP cores. We analyze our approach to show that it will not introduce any design or performance overhead. Meanwhile, study on the ITC'02 benchmark indicates that the RSN configuration can easily accommodate 10^7 to 10^{186} unique device IDs.

The rest of the paper is organized as follows. In Section II, we present the recent work on IC identification and IP fingerprinting, and highlight the novelty of our method. In Section III, we provide the background knowledge of reconfigurable scan network which is the place that we create device IDs. In Section IV, we elaborate our proposed RSN based device identification approach. Section V reports the experimental results with focus on the potential of the proposed method and its design overhead. We conclude the paper in Section VI.

II. Related Work

In this section, we will survey the literature on the following related topics: IC identification, IP fingerprinting, security applications of scan chain design and RSNs.

A. IC Identification and Authentication

Serial number is perhaps the most popular and one of the earliest ways for IC identification. A serial number can be physically indented on the device or stored permanently in the memory. However, the fact that it can be easily removed or forged makes it unsuitable to countermeasure IP theft such as illegal reproduction, redistribution, and foundry overbuilding.

Several intrinsic unclonable IC tagging schemes based on silicon manufacture variation have been proposed. In [7], a technique was created to determine a circuit's fingerprint through its glitches. In [8], the delay path variations are used to create the fingerprint for a circuit. Recently, a circuit identification method was presented in [9], where the authors embed chip IDs by replacing standard cells in the netlist with partial polymorphic gates. Upon activation of the control signal, the polymorphic gates will behave differently for certain input combinations and thus can be used to authenticate the chip. The unique challenge response pairs created by the physical unclonable functions have also been used for IC identification. These approaches are based on intrinsic fabrication variations, they cannot detect IP theft because illegally copied or over-built ICs will have different variations and hence different identifications from the original copy. Therefore, the IP cannot be traced and authenticated.

B. Digital Fingerprinting for IP Protection

IP fingerprinting was introduced to assign each copy of the design a unique fingerprint for identification. It was first reported in 1998 [10], where the authors utilized an FPGA design partitioning and tiling technique to embed distinct fingerprints in the originally watermarked design. This technique is impractical since it's only applicable to a specific structure. A generic methodology to embed fingerprints in the solutions to optimization problems was proposed in [11] where iterative optimization is applied in an incremental fashion to encode distinct fingerprints. In [12], a conceptually different methodology was proposed to construct multiple distinct copies of the design from one seed design. Unfortunately, all these as well as other early fingerprinting approaches [27] create fingerprints in the earlier stage of the VLSI design cycle, resulting in different masks, therefore, are impractical.

In [13], a satisfiability don't-care condition based circuit fingerprinting technique is developed to create fingerprints at the post-silicon stage by using MUXs to replace certain library cells. In [14], the authors proposed to utilize observability don't-care conditions and add extra wires without changing the design's functionality. In both methods, the design will be modified such that fingerprints, in the form of different layouts such as library cells and wires, can be generated at the post-silicon stage. While these methods are practical, they incur large design overhead in circuit area and delay.

In [15], a scan chain based fingerprinting scheme with easy detection and low overhead was presented. By choosing between different connection styles of adjacent scan flip flops, fingerprint bits are embedded in the scan chain. It was considered to cause no performance overhead since it made no change on the design except the scan chain. However, because the testing interface is available to the public, this method may be vulnerable.

C. Scan Chain Design and Reconfigurable Scan Networks

Scan chain is the most popular DfT technique as it provides test engineers with full controllability and observability of circuit internal states to reduce test complexity. However, scan chain also allows attackers to access sensitive information such as intellectual property or secret keys [16], [17]. To address such security concerns, a number of countermeasures have been proposed to defend against scan chain based side channel attacks. Authentication methods [18] are used to prevent unauthorized users from accessing protected data through scan chain. Nevertheless, this is not sufficient for a high-level protection since the key or password used for authentication may end up in the wrong hands. A detailed survey paper summarizing scan-based side channel attacks and corresponding countermeasures is presented in [19].

Reconfigurable scan architectures have been proposed [20] for decades. Compared to traditional scan design, RSNs allow flexible and scalable access to on-chip instrumentations in case of large scale integration, while significantly reducing test time. Recently, RSN with nearly arbitrary structure and functionality has been standardized by the IEEE P1687 [6].

The first generalized model enabling efficient formal verification and automatic generation of access patterns was presented in [21], which applies to a wide range of RSN architectures.

In this paper, we will adopt the above RSN model and utilize the different connection styles between the Segment Insertion Bit (SIB) used in the RSN by IEEE P1687 [6] to create circuit identifiers. This idea has been used to create chip watermark [22] and fingerprint [15]. We apply it to the standard industrial design interface and demonstrate its usability in providing lightweight security for embedded and IoT devices. One thing that needs to be mentioned is that IP cores are highly used, in the forms of hard IP or firm IP, in the design of embedded and IoT devices [27]. The design details of these IP cores are unavailable; therefore, the previous IP protection techniques [15, 22] cannot be applied as they require changes to be made inside the IP cores.

III. Reconfigurable Scan Networks

A. *Reconfigurable Scan Network*

Scan chains are extensively used to reduce the test complexity. They eliminate the need for sequential test pattern generation by making internal memory elements directly controllable and observable. However, in the traditional design of scan chains, where all scan registers are chained into a single scan chain, the time overhead of accessing each module's scan register can be too high. To reduce this overhead, reconfigurable scan networks are introduced, which enable dynamic reconfiguration of scan networks and allow cost-efficient access to on-chip instrumentations.

In the following, we review the definition of reconfigurable scan networks presented in [21], which covers the existing RSN standards, IEEE 1149.1-2013 [5] and IEEE P1687 (IJTAG).

An RSN has four data ports namely *scan-input*, *scan-output*, *reset input*, *clock input* as well as three control ports, *capture, shift and update* which are controlled by a 1149.1-compliant TAP [5]. RSNs are composed of *scan segments*, multiplexers or other combinational logic blocks. The scan segment consists of scan registers which are accessible through the scan-in and scan-out ports, and an optional shadow register. The state of the shadow register determines the configuration of scan networks. Scan segments provide access to testing structures and enable distributed control over the on-chip instrumentations. Each scan segment should support three modes of operations, namely *shift*, *capture* and *update*, which are controlled by external control signals.

In the capture mode, the scan registers get overwritten by the data coming from the corresponding instrument (Data-in port). During a shift operation, the data from scan-in port is shifted through the scan registers to scan-out port. In the update mode, the data in scan registers is written to the optional shadow register. Scan segment might have another control port called *select* which determines whether the scan segment can perform capture, shift and update operations.

Scan segments are connected either by buffers or *Scan Multiplexers*. The latter selects the path that scan data goes through in the network, and its select signal is referred to as *address* in the scan network literature. The internal control signals of scan segments such as *select*, and the addresses of scan multiplexers are determined by the output of combinational logic blocks whose inputs are the value of shadow registers of scan segments and the primary data and control inputs of the RSN. A scan path is *active* if all the scan segments on the path are selected, and the addresses of all on-path scan multiplexers are set appropriately. To access a scan segment in the RSN, it needs to be on an active path. A read or write access to a scan segment, as defined by IEEE 1149.1 [5], is a three-step process called a *CSU* (Capture-Shift-Update) operation: in capture mode of a *CSU*, all the scan registers on the active scan path load the test result from their corresponding instrument. Then, this data will be shifted out during the followed shift operation. Note that during shift operation, the new scan data will be shifted in as the data in scan register is being shifted out. Finally, in the update mode of a CSU, the content of scan registers on the active path gets loaded to the corresponding shadow registers.

B. *Segment Insertion Bit Based Reconfigurable Scan Network*

Segment Insertion Bit (SIB) is a hardware component proposed by IEEE P1687 [6] which can be used to reconfigure scan networks by bypassing or including scan chains in scan paths. In scan networks, SIBs are utilized to provide fine grained configurable access to scan chains of instruments and their corresponding submodules. A possible implementation of the SIB is proposed in [23] which is shown in Figure 1.

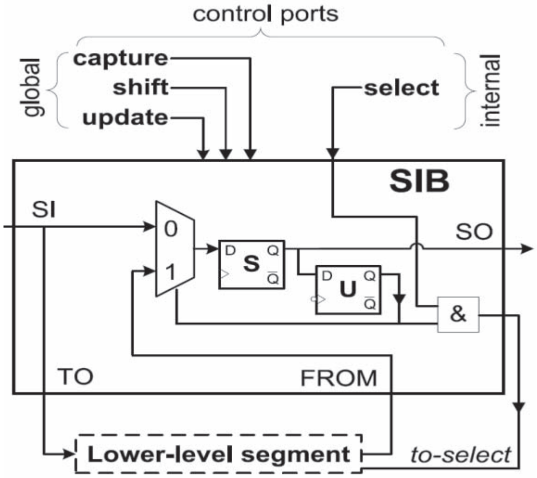

Figure 1: Implementation of a segment insertion bit [23].

An SIB has a scan-input and a scan-output as well as four control inputs, capture, shift, update and select. It also contains a 1-bit shift register *S* and a 1-bit shadow register *U*. Note that the same set of external control signals drive scan segments and SIBs in a scan network. During the shift operation, based on the value of shadow register *U* and the select signal, the data from scan-in port either gets directed to the lower level scan segment of the SIB (*Directing mode*) or bypasses the scan segment and directly goes to scan-out port (*Bypassing mode*). The value of shadow register *U* only gets updated from *S* if both *update* and *select* signals are activated. The capture operation is the same as scan segments.

The proposed IC identification scheme is based on RSNs. We will elaborate in the following section how it can be integrated in the SIB based RSNs, however, it could be applied on other implementations of RSN as well.

IV. Reconfigurable Scan Network Based IC Identification

A. Main Idea

Our IC identification scheme is built on top of the SIB-based RSNs. It takes advantage of the fact that shift register *S* and shadow register *U* in each SIB can be chained by either the Q-D or the Q'-D connection style [22, 24]. In this approach, if the Q-D connection is used to chain *S* and *U* registers, the embedded ID bit is '0', and if the Q'-D connection is used, the corresponding ID bit would be '1'. Therefore, for each SIB in the design, one identification bit can be embedded.

Suppose that the original design only uses Q-D connections for all SIBs in the RSN. Then, the chip ID of this design would be all 0s. To generate a new chip ID, the designer has the option of choosing among existing SIBs to modify their *S*/*U* connection styles. If *k* SIBs exist in the design, the designer can create unique digital IDs for up to 2^k chips.

As one might notice, when a Q'-D connection is used for *S*/*U* connection of an SIB, the negated value of *S* will be loaded to *U* during an update operation, which would make the original test inputs incorrect. Therefore, to ensure that all the instruments can be tested correctly, we need to adjust the test vectors for scan segments whose SIBs have been modified (Q'-D connection is used for their *S*/*U* registers). The adjustment only needs to be made to the test input which is shifted in during each update operation. We refer to this test input as *configuration sequence* as it determines the scan network topology after its corresponding update operation.

To adjust each configuration sequence, the following rules need to be followed for each bit in the sequence.

Rule 1. If the bit corresponds to an SIB whose *S*/*U* connection style is Q'-D, the value of this bit should be set to '0' for activating the directing mode and to '1' for enabling the bypassing mode.

Rule 2. If the bit corresponds to an SIB whose *S*/*U* connection style is Q-D, the value of this bit should be set to '1' for activating the directing mode and to '0' for enabling the bypassing mode.

These rules make sure that no matter what the style of *S*/*U* connection is in each SIB, always the correct value is stored in the shadow register and scan networks can be configured correctly. In the scan network depicted in Figure 2, suppose that the original design uses Q-D connections for all three SIBs, i.e. the design carries an ID value of '000'. In this case, to access only scan segments 1 and 3, a configuration sequence of '101' should be shifted in before the update operation. As mentioned before, this configuration sequence only works for this specific ID, and if the S/U connection style of any SIB changes, this sequence needs to be modified. For example, if an ID equal to '101' is assigned to the scan network in Figure 2, the configuration sequence for accessing scan segments 1 and 3 would be '000'.

Compared to the existing IC identification methods, our approach offers four advantages. First, it is practical as the ID bit locations in the scan network can be selected before fabrication, and the assignment of digital IDs are done at post fabrication stage. Therefore, all the designs can be fabricated with the same mask. Second, it incurs negligible overhead since the identification bits are added in the scan network, which won't affect the performance of core design. Third, it offers an additional non-destructive verification method which unlike other existing methods doesn't require depackaging of the IC. Finally, and most importantly, it does not require any scan chain information from each of the IP cores and is suitable for embedded devices.

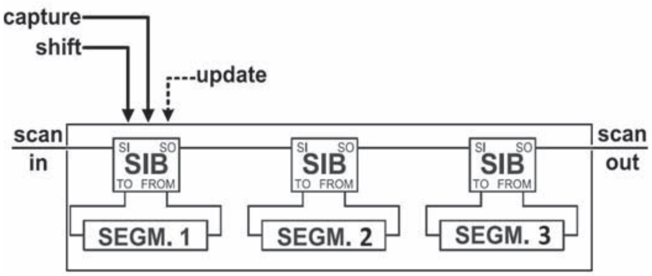

Figure 2: An example SIB based RSN for demonstrating test input adjustments.

B. Implementation

To implement the presented chip identification method, we propose to replace each original SIB in the design with a slightly different version of SIB called ID-SIB. The only change we made on the original SIB is that the connection style of ID-SIB's *S* and *U* registers can be programmed in post-fabrication stage, as shown in Figure 3. The connection programming is done by blowing up one of the two fuses of each ID-SIB in the scan network. In Figure 3, if the designer blows fuse F2, the *S*/*U* connection will be a Q-D style, and the corresponding identification bit for this ID-SIB would be '0', and if she chooses to blow the other fuse, the connection would be of Q'-D style, and the ID bit would be equal to '1'.

C. Security Analysis

To analyze the security of IC identification schemes, researchers consider two attack scenarios, ID modification and ID removal. For our chip identification scheme, the removal attack can be perceived as an instance of modification attack, for removing the chip ID, i.e. changing all the Q'-D connections in SIBs back to Q-D connections can be viewed as a modification attack targeting chip ID of all 0s. Therefore, in this section, we only focus on the ID modification attacks.

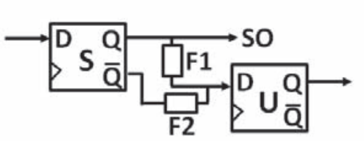

Figure 3: Programmable connections of S and U registers in ID-SIB.

In ID modification attacks, adversary's goal is to change the ID of the chip. One possible motivation for an adversary to mount these type of attacks is to resale the chip to blacklisted customers for higher prices and avoid getting detected by the chip vendor. If the digital IDs of illegally distributed chips are not modified, the identity of the rogue customer responsible for selling these chips can be easily tracked by the chip IDs.

An adversary can mount ID modification attacks, only if he is capable of depackaging, reverse engineering the chip and changing the connections of *S* and *U* registers in ID-SIBs. While we believe these assumptions about capabilities of adversaries are not realistic, especially in case of very large-scale ICs, we suggest choosing ID bits by the data integrity technique proposed in our previous work [15] to eliminate the possibility of such powerful attacks. Based on this technique, embedding ID bits for an IC is a 4 step process: (1): choose N ID bit locations, and replace the corresponding SIBs with ID-SIBs, (2): choose random values for m ID bits with $m < N$, (3): use this m-bit ID and an IC-specific key (K_{IC}) as the input to a one-way hash function to generate (N-m) bits, (4): use the final N bits as the ID bits to guide the selection of S/U connection styles at the selected ID locations. In this technique, the location of the m-bit ID and the value of the K_{IC} should be kept private to the IC vendor.

The proposed data integrity technique makes it difficult for the attacker to forge a chip ID, since a successful forgery requires knowing the value of K_{IC} and the exact location of the m-bit ID, which are only known to the IC vendor. Although it is possible for the adversary to change the connection styles between *S* and *U* registers in ID-SIBs, it will be challenging to make the correct changes that can maintain the property between ID bits.

V. Experiment Result

To validate our proposed IC identification scheme, we first see how many unique device IDs can be generated with our approach for real life circuits. Then, we discuss the design overhead.

A. Benchmark Circuits

To evaluate our identification scheme, we use the SIB based RSN benchmarks described in [21] which are based on ITC'02 SOC benchmark set [25]. Each ITC'02 benchmark circuit is specified by the modules in the SOC and their hierarchical structure, and modules are described by the numbers of their input, output, bidirectional terminals, scan chains and their lengths, test sets, and the (x, y) coordinate of their center on the SOC layout.

In the SIB based scan network benchmarks, two scan registers are designated for input and output pins of each module. In this design, doorway SIBs include or exclude lower level submodules, and instrument SIBs connect or bypass scan segments, input and output scan registers of each module from the active scan path as described in [26]. In Table 1, the details of the ITC'02 SOC benchmarks and their corresponding SIB based RSN designs are listed.

B. Potential in Creating Unique IDs

As described in section IV.A, to embed the identification bits, each SIB in the scan network needs to be replaced with an ID-SIB. Therefore, the number of potential ID bits for each chip is equal to the number of SIBs in its scan network, which is given in Table 1. As one can see in Table 1, with the exception of q127110, all the other benchmark circuits can potentially embed a good number of ID bits with the minimum of 40 bits (A586710) and maximum of 621 (P93791) ID bits, which correspond to $1.09\text{x}10^{12}$ and $8.70\text{x}10^{186}$ unique device IDs, respectively. Even in the minimum case, $1.09\text{x}10^{12}$ is a couple orders of magnitude higher than the number of devices in most of the real life embedded and IoT applications.

C. Design Overhead

The proposed IC and device identification approach has negligible performance overhead as the digital ID bits are only added in the SIBs of the scan network, which wouldn't cause any overhead to the IP core design. Moreover, the overhead incurred on testing instruments is also negligible since no extra hardware is integrated into the design, and all the changes are local which avoids rerouting. For different RSN configurations, the testing vector can be justified, which is a one-time cost, so there will no change in test coverage.

VI. Conclusion

In this paper, we propose a novel IC identification approach which, compared to other existing schemes, is more practical, has lower design overhead and provides a non-destructive verification method. This method takes advantage of the difference connection styles in the scan chain to create unique device IDs. The testing vectors will be justified accordingly to maintain the test coverage, which becomes one way for the authentication of the device ID. It can be conveniently implemented on embedded and IoT devices to utilize their testing infrastructure compliant with IEEE 1149.1-2013 and IEEE P1687 (IJTAG). Experimental results indicate that on standard benchmark circuits, we can generate unique device IDs a couple orders of magnitude higher than what typical embedded and IoT applications would need.

Acknowledgment

This work was supported by AFOSR MURI under award number FA9550-14-1-0351. Dr. Gang Qu is the corresponding author of this work.

Table 1: Characteristics of the ITC'02 Benchmarks and their corresponding SIB based Scan Networks

Designs	Characteristics of the ITC'02 Benchmarks				Number of SIBs	Number of unique device IDs
	Modules	Levels	Scan segments	Register bits		
u226	10	2	40	1,416	50	1.13E+15
d281	9	2	50	3,813	59	5.76E+17
d695	11	2	157	8,229	168	3.74E+50
h953	9	2	46	5,586	55	3.60E+16
g1023	15	2	65	5,306	80	1.20E+24
f2126	5	2	36	15,789	41	2.19E+12
q127110	5	2	21	26,158	25	3.35E+07
p228110	29	3	254	29,828	283	1.55E+85
p34392	20	3	103	23,119	123	1.06E+37
P93791	33	3	588	97,984	621	8.70E+186
T512505	31	2	128	76,846	160	1.46E+48
A586710	8	3	32	41,635	40	1.09E+12

References

[1] Christopher Clearfield Why The FTC Can't Regulate The Internet Of Things, Forbes, 18 September 2013.

[2] G. Qu and L. Yuan, “Design Things for the Internet of Things – An EDA Perspective”, IEEE/ACM International Conference on Computer Aided Design (ICCAD'14), November 2014.

[3] Joseph Steinberg. "These Devices May Be Spying On You (Even In Your Own Home)". Forbes. 27 January 2014.

[4] C. Dunbar and G. Qu, “A DTN Routing Protocol for Vehicle Location Information Protection”, Military Communications Conference (Milcom’14), October 2014.

[5] "IEEE Standard for Test Access Port and Boundary-Scan Architecture, IEEE Standard 1149.1-2013", 2013.

[6] IJTAG, “IJTAG - IEEE P1687,” Mar. 2012. [Online]. Available: http://grouper.ieee.org/groups/1687

[7] H. J. Patel, J. W. Crouch, Y. C. Kim and T. C. Kim, "Creating a unique digital fingerprint using existing combinational logic," *2009 IEEE International Symposium on Circuits and Systems*, Taipei, 2009, pp. 2693-2696.

[8] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprinting," in *Hardware-Oriented Security and Trust, IEEE International Workshop on*, Anaheim, CA, 2008.

[9] T. Wang, X. Cui et al, “A Novel Circuit Authentication Scheme based on Partial Polymorphic Gates” *in Proceedings 22th Asia and South Pacific Design Automation Conference (ASP-DAC),* 2017.

[10] . Lach, W. H. Mangione-Smith and M. Potkonjak, "FPGA Fingerprinting Techniques for Protecting Intellectual Property", *Proceedings of CI-CC*, 1998.

[11] A. E. Caldwell *et al*., "Effective iterative techniques for fingerprinting design IP," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 23, no. 2, pp. 208-215, Feb. 2004.

[12] G. Qu and M. Potkonjak, "Fingerprinting intellectual property using constraint-addition", in *Proceedings of the 37th annual ACM/IEEE Design Automation Conference*, New York, NY, 2000.

[13] C. Dunbar and G. Qu, "Satisfiability Don't Care condition based circuit fingerprinting techniques," *The 20th Asia and South Pacific Design Automation Conference*, Chiba, 2015, pp. 815-820.

[14] C. Dunbar and Gang Qu, "A practical circuit fingerprinting method utilizing observability don't care conditions," *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, San Francisco, CA, 2015, pp. 1-6.

[15] X. Chen, G. Qu, A. Cui and C. Dunbar, "Scan chain based IP fingerprint and identification," *2017 18th International Symposium on Quality Electronic Design (ISQED)*, Santa Clara, CA, 2017, pp. 264-270.

[16] B. Yang, K. Wu and R. Karri, "Secure Scan: A Design-for-Test Architecture for Crypto Chips," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 25, no. 10, pp. 2287-2293, Oct. 2006.

[17] Bo Yang, Kaijie Wu and Ramesh Karri, "Scan based side channel attack on dedicated hardware implementations of Data Encryption Standard," *2004 International Conference on Test*, 2004, pp. 339-344.

[18] S. Paul, R. S. Chakraborty and S. Bhunia, "VIm-Scan: A Low Overhead Scan Design Approach for Protection of Secret Key in Scan-Based Secure Chips," *25th IEEE VLSI Test Symposium (VTS'07)*, Berkeley, CA, 2007, pp. 455-460.

[19] J. Da Rolt, A. Das, G. Di Natale, M. L. Flottes, B. Rouzeyre and I. Verbauwhede, "Test Versus Security: Past and Present," in *IEEE Transactions on Emerging Topics in Computing*, vol. 2, no. 1, pp. 50-62, March 2014.

[20] S. Narayanan and M. A. Breuer, "Reconfigurable scan chains: A novel approach to reduce test application time," *Proceedings of 1993 International Conference on Computer Aided Design (ICCAD)*, Santa Clara, CA, USA, 1993, pp. 710-715.

[21] R. Baranowski, M. A. Kochte and H. J. Wunderlich, "Modeling, verification and pattern generation for reconfigurable scan networks," *2012 IEEE International Test Conference*, Anaheim, CA, 2012, pp. 1-9.

[22] A. Cui, G. Qu and Y. Zhang, "Ultra-Low Overhead Dynamic Watermarking on Scan Design for Hard IP Protection," in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2298-2313, Nov. 2015.

[23] R. Baranowski, M. A. Kochte and H. J. Wunderlich, "Fine-Grained Access Management in Reconfigurable Scan Networks," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 6, pp. 937-946, June 2015.

[24] S. Gupta, T. Vaish and S. Chattopadhyay, "Flip-flop chaining architecture for power-efficient scan during test application," *14th Asian Test Symposium (ATS'05)*, 2005, pp. 410-413.

[25] E. J. Marinissen, V. Iyengar and K. Chakrabarty, "A set of benchmarks for modular testing of SOCs," *Proceedings. International Test Conference*, 2002, pp. 519-528.

[26] F. G. Zadegan, U. Ingelsson, G. Carlsson and E. Larsson, "Design automation for IEEE P1687," *2011 Design, Automation & Test in Europe*, Grenoble, 2011, pp. 1-6.

[27] G. Qu and M. Potkonjak, *Intellectual Property Protection in VLSI Designs: Theory and Practice*, Kluwer Academic Publishers, ISBN 1-4020-7320-8, January 2003.